permanent legal residence. Requests for access to information in a PA system of records made by individuals who are not U.S. citizens or permanent residents will be processed under the provisions of the FOIA.

(d) *Federal contractors.* Applies to Federal contractors by contract or other legally binding action, whenever a DON contract provides for the operation, maintenance, or use of records contained in a PA system of records to accomplish a DON function.

(1) When a DON activity contracts for the operation or maintenance of a system of records or a portion of a system of records by a contractor, the record system or the portion of the record system affected are considered to be maintained by the DON activity and are subject to this subpart and subpart G of this part.

(2) The contractor and its employees are considered employees of the DON activity for purposes of the sanction provisions of the PA during the performance of the contract.

(3) The Defense Acquisition Regulatory (DAR) Council, which oversees the implementation of the Federal Acquisition Regulations (FAR) within DOD, is responsible for developing the specific policies and procedures for soliciting, awarding, and administering contracts that are subject to this subpart and 5 U.S.C. 552a.

(4) Consistent with the FAR regulations, contracts for the operation of a system of records shall identify specifically the record system and the work to be performed, and shall include in the solicitation and resulting contract the terms as prescribed by the FAR (see *http://www.privacy.navy.mil* (Admin Tools)).

(5) DON activities must furnish PA Program guidance to their personnel who solicit and award or administer Government contracts; inform prospective contractors of their responsibilities regarding the DON PA Program; and establish an internal system of contractor performance review to ensure compliance with the DON Privacy Program.

(6) This instruction does not apply to records of a contractor that are:

(i) Established and maintained solely to assist the contractor in making internal contractor management decisions, such as records maintained by the contractor for use in managing the contract;

(ii) Maintained as internal contractor employee records, even when used in conjunction with providing goods or services to a DON activity;

(iii) Maintained as training records by an educational organization contracted by a DON activity to provide training when the records of the contract students are similar to and commingled with training records of other students, such as admission forms, transcripts, and academic counseling and similar records;

(iv) Maintained by a consumer reporting agency to which records have been disclosed under 31 U.S.C. 3711; or

(7) DON activities shall establish contract surveillance programs to ensure contractors comply with the procedures established by the DAR Council.

(8) Disclosing records to a contractor for use in performing a contract let by a DON activity is considered a disclosure within DON (*i.e.*, based on an official need to know). The contractor is considered the agent of DON when receiving and maintaining the records for that activity.

(e) *Precedence.* In case of a conflict, this subpart and subpart G takes precedence over any DON directive that deals with the personal privacy and rights of individuals regarding their personal records, except for disclosure of PPI required by 5 U.S.C. 552 and implemented by Secretary of the Navy (SECNAVINST) 5720.42F.

§ 701.104 Responsibility and authority.

(a) *Delegation.* The Chief of Naval Operations (CNO) for administering and supervising the execution of 5 U.S.C. 552a, DOD Directive 5400.11 and DOD Regulation 5400.11–R. The Director, Navy Staff (DNS) will administer this program through the Head, DON PA/FOIA Policy Branch (DNS–36) who will serve as the Principal PA Program Manager for the DON.

(b) *CNO (DNS–36).* (1) Develops and implements DON policy on the provisions of the PA; serves as principal advisor on all DON PA matters; oversees the administration of the DON's PA

program; reviews and resolves PA complaints; maintains the DON's PA Online Web site; develops a Navy-wide PA training program and serves as training oversight manager; establishes, maintains, deletes, and approves Navy and joint Navy/Marine Corps PA systems of records notices; compiles reports that address the DON's PA Program to DOD and/or the Office of Management and Budget (OMB); conducts PA reviews as defined in OMB Circular A–130; publishes exempt systems of records in the CFR; and conducts staff assistance visits/program evaluations within DON to review compliance with 5 U.S.C. 552a, this subpart and subpart G of this part.

(2) Serves as PA Coordinator for the Secretary of the Navy (SECNAV), Office of the CNO (OPNAV) and the Naval Historical Center (NHC).

(3) Represents SECNAV on the Defense Privacy Board (DPO). Per DOD Directive 5400.11, the Board has oversight responsibility for implementation of the DOD Privacy Program.

(4) Represents SECNAV on the Defense Data Integrity Board. Per DOD Directive 5400.11, the Board has oversight responsibility for reviewing and approving all computer matching agreements between the DOD and other Federal, State, or local government agencies, as well as memoranda of understanding when the match is internal to DOD, to ensure that appropriate procedural and due process requirements have been established before engaging in computer matching activities.

(5) Provides input to the DPO on OMB's Federal Information Security Management Act (FISMA) Report.

(6) Coordinates on all PIAs prior to the PIA being submitted to DON CIO for review and final approval. Makes a determination as to whether the new IT system constitutes a PA system of records. If it does, determines whether an existing system covers the collection or whether a new systems notice will have to be written and approved. As necessary, assists the DON activity in creating and getting a new PA system of records notice approved.

(7) Oversees the administration of OPNAV's PA program.

(8) Chairs the DON PA Oversight Working Group.

(c) *Commandant of the Marine Corps (CMC).* (1) Administers and supervises the execution of this instruction within the Marine Corps and maintains and approves Marine Corps PA systems of records notices. The Commandant has designated CMC (ARSF) as the PA manager for the U.S. Marine Corps.

(2) Oversees the administration of the Marine Corps' PA program; reviews and resolves PA complaints; develops a Marine Corps privacy education, training, and awareness program; reviews and validates PIAs for Marine Corps information systems and submits the validation to CNO (DNS–36); establishes, maintains, deletes, and approves Marine Corps PA systems of records notices; and conducts staff assistance visits/program evaluations within the Marine Corps to review compliance with 5 U.S.C. 552a, this subpart and subpart G of this part.

(3) Serves as the PA Coordinator for all Headquarters, U.S. Marine Corps components, except for Marine Corps Systems Command and the Marine Corps Combat Development Command.

(4) Provides input to CNO (DNS–36) for inclusion FISMA Report.

(5) Serves on the DON PA Oversight Working Group.

(6) Coordinates on all PIAs prior to the PIA being submitted to DON CIO for review and final approval, making a determination as to whether the new IT system constitutes a PA system of records. If it does, determines whether an existing system covers the collection or whether a new systems notice will have to be written and approved. As necessary, assists the DON activity in creating and getting a new PA system of records notice approved.

(d) *DON CIO.* (1) Integrates protection of PPI into the overall DON major information system life cycle management process as defined in the E-Government Act of 2002 (Pub. L. 107–347).

(2) Provides guidance for effective assessment and utilization of privacy-related technologies.

(3) Provides guidance to DON officials on the conduct of PIAs (see their Web site at *http://www.doncio.navy.mil*) and oversees DON PIA policy and procedures to ensure PIAs are conducted

commensurate with the information system being assessed, the sensitivity of IIF in that system, and the risk of harm for unauthorized release of that information. Also, DON CIO reserves the right to request that a PIA be completed on any system that may have privacy risks.

(4) Reviews and approves all PIAs for the DON and submits the approved PIAs to DOD and OMB according to Federal and DOD guidance.

(5) Serves as the focal point in establishing and validating DON information systems privacy requirements and coordinating issues with other DOD Military Departments and Federal Agencies.

(6) Develops and coordinates privacy policy, procedures, education, training, and awareness practices regarding DON information systems.

(7) Compiles and prepares responses to either DOD or OMB regarding PIA issues.

(8) Develops and coordinates DON web privacy policy, education, training and an awareness program in accordance with DON Web privacy requirements including annual Web site privacy posting training with CNO (DNS–36).

(9) Provides guidance toward effective research and development of privacy-related technologies.

(10) Serves as the focal point in establishing and validating DON Web privacy requirements and coordinating issues with DOD, other Military Departments, and other Federal agencies.

(11) Provides guidance on the use of encryption software to protect privacy sensitive information.

(12) Implements DON IT privacy requirements and coordinates IT information system requirements that cross service boundaries with the Joint Staff.

(13) Provides recommended changes to CNO (DNS–36) on policy guidance set forth in this instruction regarding IT privacy policy and procedures that includes requirements/guidance for conducting PIAs.

(14) Provides input to CNO (DNS–36) for inclusion in the FISMA Report.

(15) Serves on the DON PA Oversight Working Group.

(e) *The Chief of Information (CHINFO) and U.S. Marine Corps Director of Public Affairs (DIRPA).* CHINFO and DIRPA, in accordance with DON CIO guidance on Department-wide Information Management (IM) and IT matters, are responsible for developing and administering Navy and Marine Corps Web site privacy policies and procedures respectively per SECNAVINST 5720.47B. Additionally, CHINFO and DIRPA:

(1) Maintains master World Wide Web (WWW) page to issue new service-specific Web privacy guidance. CHINFO will maintain a master WWW page to issue DON guidance and DIRPA will link to that page. All significant changes to this Web site and/or its location will be issued via Naval (ALNAV) message.

(2) Maintains overall cognizance for DON and U.S. Marine Corps Web sites and Web site content-related questions as they pertain to Web site privacy requirements.

(3) Ensures that public-facing Web sites have machine-readable privacy policies (*i.e.*, web privacy policies are P3P-enabled or automatically readable using some other tool).

(4) Provides input to CNO (DNS–36) for inclusion in the FISMA Report.

(5) Serves on the DON PA Oversight Working Group.

(f) *DON PA Oversight Working Group.* The DON PA Oversight Working Group is charged with reviewing and coordinating compliance with DON PA program initiatives. CNO (DNS–36) will chair this working group, hosting meetings as deemed appropriate to discuss best PA practices, PA issues, FISMA reporting and other reporting requirements, PA training initiatives, etc. At a minimum, membership shall consist of CNO (DNS–36), DON CIO, CMC (ARSF), CMC (C4I–IA), OJAG (Code 13), OGC (PA/FOIA), CMC (JAR), CHINFO, and CMC (PA).

(g) *DON activities.* Each DON activity is responsible for implementing and administering a PA program under this subpart and subpart G.

(h) *Navy Echelon 2 and 3 Commands and Marine Corps Major Subordinate Commands.* Each Navy Echelon 2 and 3 Command and Marine Corps Major Subordinate Command will designate a PA Coordinator to:

(1) Serve as principal point of contact on PA matters.

(2) Advise CNO (DNS–36) promptly of the need to establish a new Navy PA system of records; amend or alter an existing Navy system of records; or, delete a Navy system of records that is no longer needed.

(3) Advise CMC (ARSF) promptly of the need to establish a new Marine Corps PA system of records; amend or alter an existing Marine Corps system of records; or, delete a Marine Corps system of records that is no longer needed.

(4) Ensure no official files are maintained on individuals that are retrieved by name or other personal identifier without first ensuring that a system of records notice exists that permits such collection.

(5) Ensure that PA systems of records managers are properly trained on their responsibilities for protecting PPI being collected and maintained under the DON PA Program.

(6) Provide overview training to activity/command personnel on the provisions of this subpart and subpart G.

(7) Issue an implementing instruction which designates the activity's PA Coordinator, addresses PA records disposition, addresses PA processing procedures, identifies those PA systems of records being used by their activity; and provide training/guidance to those personnel involved with collecting, maintaining, disseminating information from a PA system of records.

(8) Review internal directives, forms, practices, and procedures, including those having PA implications and where Statements (PAS) are used or PPI is solicited.

(9) Maintain liaison with records management officials (e.g., maintenance and disposal procedures and standards, forms, and reports), as appropriate.

(10) Provide guidance on handling PA requests; scope of PA exemptions; and the fees, if any, that may be collected.

(11) Conduct staff assistance visits or program evaluations within their command and lower echelon commands to ensure compliance with the PA.

(12) Work closely with their PA systems managers to ensure they are properly trained with regard to collecting, maintaining, and disseminating information in a PA system of records notice.

(13) Process PA complaints.

(14) Ensure protocols are in place to avoid instances of loss of PPI. Should a loss occur, take immediate action to apprise affected individuals of how to ensure their identity has not been compromised.

(15) Work closely with their public affairs officer and/or web master to ensure that PPI is not placed on public Web sites or in public folders.

(16) Annually conduct reviews of their PA systems of records to ensure that they are necessary, accurate, and complete.

(17) Provide CNO (DNS–36) or CMC (ARSF) respectively, with a complete listing of all PA Coordinators under their jurisdiction. Such information should include activity name, complete mailing and E-Mail addresses, office code, name of PA Coordinator, and commercial, DSN, and FAX telephone numbers.

(18) Review and validate PIAs for their information systems and submit the validation to CNO (DNS–36) for Navy information systems or to HQMC (ARSF) for Marine Corps information systems.

(i) *DON employees/contractors.* DON employees/contractors are responsible for safeguarding the rights of others by:

(1) Ensuring that PPI contained in a system of records, to which they have access or are using to conduct official business, is protected so that the security and confidentiality of the information is preserved.

(2) Not disclosing any information contained in a system of records by any means of communication to any person or agency, except as authorized by this instruction or the specific PA systems of records notice.

(3) Not maintaining unpublished official files that would fall under the provisions of 5 U.S.C. 552a.

(4) Safeguarding the privacy of individuals and confidentiality of PPI contained in a system of records.

(5) Properly marking all documents containing PPI data (e.g., letters, E-Mails, message traffic, etc.) as ''FOR OFFICIAL USE ONLY—PRIVACY

SENSITIVE—Any misuse or unauthorized disclosure can result in both civil and criminal penalties.''

(6) Not maintaining privacy-sensitive information in public folders.

(7) Reporting any unauthorized disclosure of PPI from a system of records to the applicable Privacy Point of Contact (POC) for his/her activity.

(8) Reporting the maintenance of any unauthorized system of records to the applicable Privacy POC for his/her activity.

(j) *Denial authority*. Within DON, the head of the activity having cognizance over an exempt PA system of record is authorized to deny access to that information under the exemptions cited in the PA systems of records notice. The denial authority may also deny requests to amend a system of records or to deny notification that a record exists. As deemed appropriate, the head of the activity may further designate initial denial authority to an individual properly trained on the provisions of the PA and this subpart and subpart G of this part.

(k) *Release authority*. Within DON, officials having cognizance over a nonexempt PA system of record that is requested by a first party or his/her authorized representative are authorized to release records. A release authority may also grant requests for notification and amendment of systems of records. The PA systems manager, who is properly trained on the provisions of 5 U.S.C. 552a, DOD Directive 5400.11 and DOD 5400.11–R, may be delegated this responsibility.

(l) *Review authority*. (1) Assistant Secretary of the Navy (Manpower & Reserve Affairs) (ASN(M&RA)) is designated to act upon requests for administrative review of initial denials of requests for amendment of records related to fitness reports and performance evaluations of military personnel.

(2) Both the JAG and GC are designated to act upon requests for administrative review of initial denials of records for notification, access, or amendment of records under their cognizance.

(3) The authority of SECNAV, as the head of an agency, to request records subject to the PA from an agency external to DOD for civil or criminal law enforcement purposes, under (b)(7) of 5 U.S.C. 552a, is delegated to CMC; the Commander, Naval Criminal Investigative Service; JAG and GC.

(m) *System manager*. System managers are responsible for overseeing the collection, maintenance, use, and dissemination of information from a PA system of records and ensuring that all personnel who have access to those records are aware of their responsibilities for protecting PPI that is being collected or maintained. In this capacity, they shall:

(1) Establish appropriate administrative, technical, and physical safeguards to ensure the records in every system of records are protected from unauthorized alteration, destruction, or disclosure.

(2) Protect the records from reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

(3) Work closely with their coordinator to ensure that all personnel who have access to a PA system of records are properly trained on their responsibilities under the PA. Training materials may be downloaded from *http://www.privacy.navy.mil*.

(4) Ensure that no illegal files are maintained.

NOTE: Official files on individuals that are retrieved by name and/or personal identifier must be approved and published in the FEDERAL REGISTER.

(5) Review annually each PA system of records notice under their cognizance to determine if the records are up-to-date and/or used in matching programs and whether they are in compliance with the OMB Guidelines. Such items as organization names, titles, addresses, etc., frequently change and should be reported to CNO (DNS–36) for updating and publication in the FEDERAL REGISTER.

(6) Work with IT personnel to identify any new information systems being developed that contain PPI. If a PA systems notice does not exist to allow for the collection, assist in creating a new systems notice that permits collection.

(7) Complete and maintain a PIA for those systems that collect, maintain or

disseminate IIF, according to DON PIA guidance found at *http://www.privacy.navy.mil* and *http://www.doncio.navy.mil*.

(8) Complete and maintain a disclosure accounting form for all disclosures made without the consent of the record subject, except those made within DOD or under FOIA. (See 701.111).

(9) Ensure that only those DOD/DON officials with a ''need to know'' in the official performance of their duties has access to information contained in a system of records.

(10) Ensure safeguards are in place to protect the privacy of individuals and confidentiality of PPI contained in a system of records.

(11) Ensure that records are maintained in accordance with the identified PA systems of records notice.

(12) Ensure that each newly proposed PA system of records notice is evaluated for need and relevancy and confirm that no existing PA system of records notice covers the proposed collection.

(13) Stop collecting any category or item of information about individuals that is no longer justified, and when feasible remove the information from existing records.

(14) Ensure that records are kept in accordance with retention and disposal requirements set forth in SECNAVINST 5720.47B.

(15) Take reasonable steps to ensure the accuracy, relevancy, timeliness, and completeness of a record before disclosing the record to anyone outside the Federal Government.

(16) Identify all systems of records that are maintained in whole or in part by contractor personnel, ensuring that they are properly trained and that they are routinely inspected for PA compliance.

§ 701.105 Policy.

DON recognizes that the privacy of an individual is a personal and fundamental right that shall be respected and protected and that PPI shall be collected, maintained, used, or disclosed to ensure that it is relevant and necessary to accomplish a lawful DON/DOD purpose required to be accomplished by statute or Executive Order (E.O.). Accordingly, it is DON policy that DON activities shall fully comply with 5 U.S.C. 552a, DOD Directive 5400.11 and DOD 5400.11–R to protect individuals from unwarranted invasions of privacy when information is collected, processed, maintained, or disseminated. To ensure compliance, DON activities shall follow the procedures listed in this section.

(a) *Collection, maintenance and use.* (1) Only maintain systems of records that have been approved and published in the FEDERAL REGISTER. (See *http://www.privacy.navy.mil* for a list of all DOD, Navy, Marine Corps, and component systems of records notices, as well as, links to Government-wide systems that the DON is eligible to use).

NOTE: CNO (DNS–36) can assist Navy activities in identifying existing systems that may meet their needs and HQMC (ARSF) can assist Marine Corps activities.

(2) Only collect, maintain, and use PPI needed to support a DON function or program as authorized by law or E.O. and disclose this information only as authorized by 5 U.S.C. 552a, this subpart and subpart G of this part. In assessing need, DON activities shall consider alternatives such as: truncating the SSN by only using the last four digits; using information that is not individually identifiable; using a sampling of certain data for certain individuals only. Additionally, they shall consider the length of time the information is needed and the cost of maintaining the information compared to the risks and adverse consequences of not maintaining the information.

(3) Only maintain PPI that is timely, accurate, complete, and relevant to the purpose for which it was collected.

(4) DON activities shall not maintain records describing how an individual exercises his/her rights guaranteed by the First Amendment (freedom of religion; freedom of political beliefs; freedom of speech; freedom of the press; the right to peaceful assemblage; and petition for redress of grievances), unless they are: expressly authorized by statute; authorized by the individual; within the scope of an authorized law enforcement activity; or are used for the maintenance of certain items of information relating to religious affiliation for members of the naval service who are chaplains.